AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method for establishing a secure connection between a client platform and a service, said client having a virtual machine and knowing and trusting a first public key, said method comprising:

downloading a digitally signed applet ~~from the service~~ to the client platform, said applet comprising code that is executable on the client platform virtual machine to cause the client platform to store a second public key that allows authentication between the client platform and the service;

a'

before the client platform virtual machine executes the digitally signed applet, verifying the digitally signed applet at the client platform using ~~a~~ the first public key the client platform already knows and trusts;

executing the downloaded applet code ~~at~~ with the client platform virtual machine, thereby ~~controlling~~ causing the client platform to store a second public key corresponding to the ~~server~~service; and

using the stored second public key to authenticate the service and establish the secure connection.

2. (currently amended) The method of claim 1 wherein the applet includes a second public key payload and further includes first program code that controls the client platform to store the second public key to a non-volatile memory.

3. (currently amended) The method of claim 2 wherein the non-volatile memory comprises a disk.

4. (original) The method of claim 2 wherein the applet further includes second program code that controls the client platform to use the stored second public key to verify a signature subsequently provided by the server.

5. (original) The method of claim 1 wherein the applet further includes program code that controls the client platform to use the stored second public key to verify a signature subsequently provided by the server.

6. (currently amended) The method of claim 1 wherein the executing step includes controlling the client platform virtual machine to store, at the client, a second public key in the form of a digital certificate corresponding to the server, and the using step comprises receiving a digital signature from the server, and authenticating the received digital signature under control of the executing applet through use of the stored digital certificate corresponding to the server.

7. (original) The method of claim 1 wherein the using step includes having the executing applet invoke a further applet to establish a secure connection.

8. (currently amended) The method of claim 1 wherein the applet comprises a signed ~~Java~~ Archive containing a digital certificate corresponding to the server, and a program fragment that stores the digital certificate in a predetermined location on the client platform that permits the client platform to later retrieve the stored digital certificate.

9. (currently amended) A client platform for establishing a secure connection with a service over a network, said client platform having a virtual machine and knowing and trusting a first public key, said client platform comprising:

an applet receiver that receives a digitally signed applet from the service over the network, said applet being executable by the client platform virtual machine to cause the client platform to store a second public key that allows authentication between the client platform and the service;

wherein the client platform virtual machine includes an applet verifier that, before executing the applet, verifies the digitally signed applet using a first public key the client platform already knows and trusts;

wherein the client platform virtual machine further includes an applet executor that executes the applet, thereby controlling the client platform to store a second public key corresponding to the server, and uses the stored second public key to authenticate the service and establish the secure connection.

10. (currently amended) A method for establishing a secure connection with a client platform virtual machine, comprising:

downloading an executable applet to the client platform virtual machine, the digitally signed applet being digitally signed such that the client platform virtual machine can verify the digitally signed applet using a first public key the client platform already knows and trusts, the digitally signed applet including a second public key and code

executable by the client platform virtual machine that controls the ~~applet~~ client platform virtual machine to store the second public key on the client platform;

sending a digital credential to the client, said digital credential being verifiable by the client platform using the stored second public key; and

establishing a secure communication with the client based on said digital credential as verified by the client.

11. (original) The method of claim 10 wherein the applet code controls the client platform to store the second public key to a non-volatile memory.

12. (currently amended) The method of claim 11 wherein the non-volatile memory comprises a disk.

13. (original) The method of claim 10 wherein the applet further includes further code that controls the client platform to use the stored second public key to verify the digital credential.

14. (original) The method of claim 10 further including sending a further applet to the client platform in response to an invocation of the further applet by the first-mentioned applet.

15. (currently amended) The method of claim 10 wherein the applet comprises a signed ~~Java~~ Archive containing a digital certificate, and a program fragment that stores the digital certificate in a predetermined location on the client platform that permits the client platform to later retrieve the stored digital certificate.

16. (currently amended) A server for establishing a secure connection with a client over a network, said client having a virtual machine and knowing and trusting a first public key, said server comprising:

an applet transmitter that transmits a digitally signed applet to the client over the network, the applet being digitally signed using ~~a~~ the first public key the client already knows and trusts, the applet being executable by the client virtual machine to control ~~including a program that controls~~ the client to store a second public key corresponding to the server; and

a digital credential transmitter that transmits a digital credential to the client executing the applet, the digital credential being authenticatable by the client using the second public key.

17. (currently amended) A method for establishing a secure connection between a server and a web browser having access to a first, trusted public key and also having a virtual machine, comprising:

downloading a digitally signed ~~item~~ applet including executable code from the server to the browser, the ~~item~~ applet including a second public key;

verifying the digitally signed ~~item~~ applet at the browser using the first public key;

executing the applet with the virtual machine to cause the client to store ~~storing~~ the second public key into a certificate store associated with the browser in response to the verifying step; and

using the stored second public key to authenticate the server.

a1

18. (currently amended) A method as in claim 17 wherein the ~~item~~ applet comprises an ~~Java~~ archive.